

1. An apparatus for sealing a data repository to a trusted computing platform, the apparatus comprising:

an embedded security system (ESS) comprising at least one platform configuration register;

a measurement module configured to generate a measurement value for a device physically connected to a computer system and to extend the measurement value to at least one platform configuration register; and

a key management module configured to seal a cryptographic key associated with a data repository to the value in at least one platform configuration register and to unseal the cryptographic key by way of the ESS.

2. The apparatus of claim 1, further comprising a cryptographic module configured to encrypt data stored to the data repository and to decrypt data read from the data repository with the cryptographic key.

3. The apparatus of claim 1, wherein the ESS is a Trusted Platform Module (TPM) in accordance with the Trusted Computing Group computer system specification.

4. A system for sealing a data repository to a trusted computing platform, the system comprising:

a data repository configured to encrypt data written to the data repository and to decrypt data read from the data repository using a cryptographic key;

an embedded security system (ESS) comprising at least one platform configuration register;

a measuring module configured to generate a measurement value for a device within the system and to extend the measurement value to one of the at least one platform configuration registers; and

a key management module configured to seal a cryptographic key associated with a data repository to the at least one platform configuration register value and to unseal the cryptographic key by way of the ESS.

5. The system of claim 4, wherein the ESS is a Trusted Platform Module (TPM) in accordance with the Trusted Computing Group computer system specification.

6. The system of claim 4, wherein the key management module is further configured to write the sealed cryptographic key to a non-volatile data repository and to read the sealed cryptographic key from a non-volatile data repository.

7. The system of claim 6, wherein the non-volatile data repository is a repository selected from the group consisting of an unencrypted partition of a hard drive, a removable device, and a removable media.

8. The system of claim 4, wherein the key management module is configured to read a sealed cryptographic key, unseal the cryptographic key, and provide the cryptographic key to the data repository before an operating system loads.

9. A computer readable storage medium comprising computer readable code configured to carry out a method for sealing a data repository to a trusted computing platform, the method comprising:

encrypting data on a data repository with a cryptographic key;
sealing the cryptographic key to a platform configuration to
produce a sealed key;
unsealing the sealed key to produce the cryptographic key; and
decrypting data on the data repository with the cryptographic key.

10. The computer readable storage medium of claim 11, wherein sealing comprises generating a measurement value for a device comprising the platform configuration and generating the sealed key with the measurement value.

11. The computer readable storage medium of claim 12, wherein generating a measurement value comprises hashing a code image.

12. The computer readable storage medium of claim 12, wherein the sealed key is generated with a Trusted Platform Module (TPM).

13. The computer readable storage medium of claim 11, wherein unsealing comprises decrypting the sealed key with a measurement value for a device comprising the platform configuration, the measurement value matching a measurement value used to produce the sealed key.

14. The computer readable storage medium of claim 15, wherein a TPM unseals the sealed key.

15. The computer readable storage medium of claim 11, further comprising storing the sealed cryptographic key in a removable device.

16. The computer readable storage medium of claim 11, wherein the platform configuration comprises a serial number for the data repository, .

17. The computer readable storage medium of claim 11, wherein the platform configuration comprises a decryption module.

18. The computer readable storage medium of claim 11, wherein the platform configuration comprises firmware and software accessible to a processor without the sealed key.

19. A method for sealing a data repository to a trusted computing platform, the method comprising:

encrypting data on a data repository with a cryptographic key;
sealing the cryptographic key to a platform configuration to
produce a sealed key;
unsealing the sealed key to produce the cryptographic key; and
decrypting data on the data repository with the cryptographic key.

20. The method of claim 21, wherein sealing comprises generating a measurement value for a device comprising the platform configuration and generating the sealed key with the measurement value.

21. The method of claim 22, wherein generating a measurement value for a device comprises hashing firmware code for the device.

22. The method of claim 22, wherein the sealed key is generated with a Trusted Platform Module (TPM).

23. The method of claim 21, wherein unsealing comprises decrypting the sealed key with a measurement value for a device comprising the platform configuration, the measurement value matching a measurement value used to produce the sealed key.

24. The method of claim 21, wherein a TPM unseals the sealed key.

25. The method of claim 21, further comprising storing the sealed key in a removable device.

26. The method of claim 21, wherein the platform configuration comprises a serial number for the data repository.

27. The method of claim 21, wherein the platform configuration comprises a decryption module.

28. The method of claim 21, wherein the platform configuration comprises firmware and software accessible to a processor without the sealed key.

29. An apparatus for sealing a data repository to a trusted computing platform,
the apparatus comprising:

means for generating a measurement value for a device among a
plurality of devices comprising a platform configuration;

means for sealing a cryptographic key associated with a data
repository to the measurement value representing the device to produce a
sealed key; and

means for unsealing the sealed key.

30. An apparatus for sealing a data repository to a trusted computing platform, the apparatus comprising:

an embedded security system (ESS) comprising at least one platform configuration register and configured to seal a cryptographic key to platform configuration data stored in the at least one platform configuration register to produce a sealed key and further configured to unseal the sealed key to re-produce the cryptographic key;

a key management module configured to direct the ESS to seal a cryptographic key associated with a data repository to a measurement value associated with the data repository and further configured to manage the sealed key,

a measurement module configured to generate the measurement value for the data repository physically connected to the ESS, the ESS extending the measurement value to the at least one platform configuration register;

a cryptographic module configured to encrypt data stored to the data repository and to decrypt data read from the data repository with the cryptographic key, and

a removable data repository configured to store the sealed key associated with the data repository.